UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/029,349	12/28/2001	Leon Hurst	004770.00756	5493

22907 7590 06/27/2006

BANNER & WITCOFF
1001 G STREET N W
SUITE 1100
WASHINGTON, DC 20001

EXAMINER	
ZAND, KAMBIZ	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/029,349	HURST ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,16-27,72,76-78 and 82-94* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,16-27,72,76-78 and 82-94* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 11-15, 28-71, 73-75 and 79-81 have been cancelled.
4. Claims 1, 6-10, 16, 19-27, 72, 77 and 82 have been amended.
5. new claims 84-94 have been added.
6. Claims 1-10, 16-27, 72, 76-78 and 82-94 are pending.
7. Examiner withdraws rejection of claims 1-10 and 82 under 35 U.S.C 112-second paragraphs due to correction by the applicant(s).
8. The rejections of claims 11-15 under 35 U.S.C 112-second are moot due to cancellation of the claims by the applicant(s).
9. The double patenting rejection of claim 76 is moot due to cancellation of claim 75 by the applicant(s).

Claim Objections

10. **Claims 6-10** objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is

required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

11. **Examiner suggests that claims 6-10 should be written independent of claims 1-5 since they do not represent method claims in contradiction with their dependencies on the base method claims and the dependent intervening method claims.**

Response to Arguments

12. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

Double Patenting

13. **Claim 77** is objected to under 37 CFR 1.75 as being a substantial duplicate of claim 76. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k). both claims are identical depending on the same claim (72).

Claim Rejections - 35 USC § 102

14. **Claims 1-10, 16-27 and 84-94** are rejected under 35 U.S.C. 102(e) as being anticipated by DeMello et al (6,891, 953 B1).

As per claim 1 DeMello et al (6,891, 953 B1) teach a method of decrypting encrypted content stored on a terminal, the method comprising the steps of: **receiving a request to access encrypted content on a terminal (see col.2, lines 4-8 where it disclosed the protected content are encrypted in harmony with col.3, lines 18-33 where a request for such access is being disclosed)**; obtaining a license comprising a content decryption key (see col.6, lines 46-53) and a set of binding attributes, the attributes including a public key (see col.6, lines 36-67; col.7, lines 1-2) **of an authorized user of the encrypted content (see col.6, lines 42-45 where examiner considers the user activation certificate corresponding to applicant's "the authorized user"); in response to the request, polling a personal trusted device of said user to digitally sign data with a private key associated with the device (see col.11, lines 48-55 where examiner considers the server corresponding to applicants personal trusted device use the private key of the fulfillment center which is the database of the server provider and is associated with the sever to sign); and receiving said digitally signed data from said device (see col.11, lines 50-67; col.12, lines 1-17 where data is received and authenticated)**; verifying at the terminal the digitally signed data utilizing the said public key; and wherein the terminal in response to verification of the digitally signed data uses the content decryption key to decrypt the encrypted content (see fig.2-4 and associated text; col.11, lines 43-67; col.8,

lines 1-6; col.21, lines 36-67; col.22-28; col.33, lines 28-67 disclose all above limitations including certification of the license with user's attributed including the keys, verification of signed certificate; hashing verification to tamperproof the content and communication between the two parties including the decryption of the content by the receiver by decryption key).

As per claims 2 DeMello et al (6,891, 953 B1) teach a method as claimed in claim 1 comprising: encrypting at least the content decryption key (see col.2, lines 22-30; col.6, lines 38-46 where the decryption key which is the same as encrypted key because they are symmetric keys are encrypted).

As per claim 3 DeMello et al (6,891, 953 B1) teach a method as claimed in claim 2, wherein: encryption is performed using a public key of an asymmetric key pair such that decryption of the content decryption key is carried out using a private key of the asymmetric key pair (see col.2, lines 61-67;col.3, lines 1-2;col.6, lines 10-21 and col.11, lines 49-57).

As per claim 4 DeMello et al (6,891, 953 B1) teach a method as claimed in claim 3, wherein: the private key is stored in a tamperproof and secure location (see col.6, lines 10-21;col.10, lines 30-44 and col.11, lines 33-44).

As per claims 5 and 18 DeMello et al (6,891, 953 B1) teach a method, a terminal as claimed in claims 4, 17 respectively, wherein: the secure location comprises a security element (see col.14, lines 7-16 where the ids corresponds to applicant's security elements).

As per claims 6-10 DeMello et al (6,891, 953 B1) teach a computer readable medium storing computer executable instructions for performing the method according to claims 2-5 respectively and are rejected for same reasons than claims 2-5 above in addition to col.29-39 where the instructions for executing such limitations are outlined; col.7, lines 38-42).

Examiner suggests that claim 6 be introduced as an independent claim and claims 7-10 be introduced as the dependent claim of claim 6.

As per claim 16 DeMello et al (6,891, 953 B1) teach a terminal which renders encrypted content comprising:

a storage for the encrypted content and a license (see col.6, lines 45-47 the DRAM and 53-67), the license containing a content decryption key and a set of binding attributes, the attributes including a public key for a licensee of said content (see col.6, lines 36-67; col.7, lines 1-2);

a protected processing environment (see fig.1 and associated text; col.1, lines 60-67);

a network interface which, in response to said terminal receiving a request to access said stored encrypted content (see fig.2 and associated text; see col.2, lines 1-61),

establishes a communication link between the terminal and at least one other terminal (see fig.2 and associated text) to request the other terminal to encrypt and digitally sign identity verification data using a private key stored at the other terminals and which delivers the digitally signed identity verification data received from the other terminal to the protected processing environment (see fig.2-4 and associated text; col.11, lines 43-67; col.8, lines 1-6; col.21, lines 36-67; col.22-28; col.33, lines 28-67 disclose all above limitations including certification of the license with user's attributed including the keys, verification of signed certificate; hashing verification to tamperproof the content and communication between the two parties including the decryption of the content by the receiver by decryption key); and

wherein the protected processing environment uses said public key to decrypt said encrypted identity verification data, compares said decrypted data with said digital signature to verify the digitally signed data, and upon successful verification of the digitally signed data, the protected processing environment decrypts the encrypted content using the content decryption key (see fig.7-8 and associated text and as applied to claim 1 above).

As per claim 17 DeMello et al (6,891, 953 B1) teach a terminal as claimed in claim 16, comprising: a tamperproof and secure storage for private key of an asymmetric key pair: and wherein the protected processing environment decrypts at least the content decryption key, the content decryption key having been encrypted using a public key of

the asymmetric key pair (see col.2, lines 22-30 and 61-67;col.3, lines 1 and 2;col.6, lines 10-21 and 30-44; col.11, lines 33-57).

As per claims 19-21 DeMello et al (6,891, 953 B1) teach a terminal as claimed in claims 16, 17 and 18 respectively, wherein: the digitally signed identity verification data is delivered to the storage (see col.6, lines 45-47 and 53-67 DRAM).

As per claims 22-27 DeMello et al (6,891, 953 B1) teach a terminal as claimed in claims 16-21 respectively, wherein: the network interface issues a request to the other terminal to provide/request the digitally signed identity verification data (see fig.2-4 and associated text; col.6-28).

Claim 72 limitations are rejected based on similar limitations according to claims 1 and 16 above. In addition see DRM operates in both secure and non-secure based on the security level as disclosed on col.6-12.

As per claim 76 DeMello et al (6,891, 953 B1) teach a terminal in accordance with claim 72 wherein: an encrypted part of the license includes a user identity certificate issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content (see col.6, lines 36-53; col.7).

As per claims 78 and 82-83 DeMello et al (6,891, 953 B1) teach URL disclosure of the limitations (see col.11, lines 33-45 and col.9, lines 5-63).

As per claims 84 and 94 A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). DeMello et al (6,891,953 B1) clearly disclose the process in a network environment as supported in fig.1-8 and col.7, lines 14-51; col.8, lines 6-19; col.5, lines 57-63). Therefore is the terminal is device of the licensee as applied to claims 1 and 16 above then the mobile phone is only another terminal design in that respect performing the same process as disclosed by DeMello.

As per claims 85-86 DeMello disclose communication via network interface as disclosed in fig.1-4 and associated text including using wireless interface. Also see Col.5, lines 58-63 disclose using such device as PDA, Pocket PC. A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)).

As per claim 87 DeMello et al (6,891, 953 B1) teach the method of claim 1, wherein said terminal is rendering machine, and said method further includes a step of rendering said decrypted content on said rendering machine (see col.6-9).

As per claim 88-89 DeMello et al (6,891, 953 B1) teach the method of claim 1, further comprising the steps of receiving an identification of a user making said request; and comparing said identification with a public portion of said license; and accessing in order to locate a license corresponding to the use (see col.2, lines 50-61; col.5, lines 23-27; and fig.1-8 and associated text see databases).

As per claim 92 DeMello et al (6,891, 953 B1) teach a hashing of data and signature and comparing the hashing for verification (see col.6, lines 53-67; col.11, lines 43-67; col.8, lines 1-6; col.21, lines 36-67; col.22-28; col.33, lines 28-67 disclose, verification of signed certificate; hashing verification to tamperproof the content and communication between the two parties including the decryption of the content by the receiver by decryption key).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. **Claims 90-91 and 93** are rejected under 35 U.S.C. 103(a) as being unpatentable over DeMello et al (6,891, 953 B1).

DeMello disclose all limitation of the claims as applied to the claims above but do not expressly disclose random generation of the data. However Rosen (5,557,518 A) teach random generation of the data by a device (see fig.9b and associated text). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Rosen's random number generator device in DeMello's secure content distribution in order to have customer communication and authentication in a secure manner by changing the authentication parameters randomly.

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KAMBIZ ZAND
PRIMARY EXAMINER

06/23/2006

AU 2132